עבודה סופית "מבוא להגנת סייבר"

- **שם סטודנט :**

מסעוד גאנם .

- **שם מרצה :**

רעיה חזי .

- **שם קורס :**

תקשורת נתונים ואבטחת מידע – מבוא להגנת סייבר

תשף_ב_5441044

- **נשוא :**

אבטחת אתרים .

- **כלי עזר :**

ויקיפידיה , הרצאות ביוטיוב, קורס שאני עושה בהקשר לאבטחת מידע

ופיתוח אתרים

ביבליוגרפיה	עמוד 1
מה הוא אתר אינטרנט ?	עמוד -2
ממה אתר מורכב ?	עמוד -3
סיבות בניה אתרים	עמוד 3-4
תקיפה SQL לאינטרנט	עמוד -5
אפשריות להתגוננות מתקיפה SQL	עמוד -6
תקיפה XSS	עמוד -7
טבלה כלים שיימושים לבנית וקידום אתרים	עמוד -8
כלים/שיטות תקיפות נפוצות	עמוד -9
שומרים על אתרים וחשבונות מפריצות והשתלטות	עמוד 10-11

אבטחת אתרים .

מה הוא אתר אינטרנט ?

אתר האינטרנט הוא אתר שמורכב או אוסף של דפי אינטרנט , ולפעמים משאבים נוספים , המקושרים בניהם ולרוב שותפים לשם תחום מסוים, וניתנים לגישה דרך רשת האינטרנט .

ברוב הפעמים מדבור בדפים המוחזרים כולם על אותו השרת , אתר עשוי להתארח על גבי כמה שרתים , הרבה אתרים מאוחסנים אצל ספקי השירות אירוח האתרים .

אתרי האינטרנט מנוהלים על ידי גורם אחד יחיד שהו מנהל האתר או בונה האתר .

היום יש כחצי או יותר מיליארד אתרי אינטרנט בעולם בעלי שם תחום , מכלול אתרי האינטרנט הזמינים לציבור נקרא באנגלית (**'World Wide Web'**) והיא רשת כלל עולמית או בראשי תיבות שהם **WWW** .

אתר אינטרט הוא תמונת הראי אל מול עולם של צרכנות ומדיה, תקשורת המונים של צרכנים לצרכנים אחרים, וחיפוש מתמיד אחר שרותים ומוצרים.

לאחר קניית דומיין מתאים ובחירת אחסון אתרים ייעודי לצורך העניין, כל שנותר הוא שיהיה לנו אתר אינטרנט. ישנו מבחר רב של אתרי אינטרנט החל מדף נחיתה בודד דרך אתר תדמית המפיץ את הבשורה וכלה באתר מכירות אונליין.

ממה האתר מורכב ?

הרכבו של אתר הוא הדפים של אתר האינטרנט שהם כתובים בקוד המבוסס על תקנים ה"HTML" או התקן "XHTML" ולרוב נעשה שימוד ב CSS שזה **"**Cascading Styles Sheets" ובעברית זה
גלינוצ עיצוב מדורגים , לשם עיצוב דף האינטרנט .
אפשר לשלב באתר שאנחנו בונים תוכם דינמי ואינטראקטיבי בעזרת קוד בשפת ה **JavaScript** , שהיא מובנת או ממומשת ברוב הדפדפנים ויש לנו עוד שפות שאפשר להשתמש בהם כמו **VBScript**של חברה מיקרוסופט , כשכבה נוספת על גבי קוד ה **HTML** שנמצא בדפיו של האתר .
לפעמים נשתמש בטכנולוגיות צד שרת כמו **PHP & ASP & Node**.js , השימוש בהן זה שהקוד מתורגם כבר בשרת האתר , ישר או מיד עם קבלת בקשה הדף מהמשתמש , והוא מייצר קוד HTML שהדפדפן של המשתמש יוכל להציג .
לעיתים קובות השימוש בטכנולוגיות האלה נשתמש כדי לשלב מידע מתוך בסיס נתונים שנמצא על השרת .
דפדפן כולל בדרל כלל פלאג-אין-ים המאפשרות הצגת תוכן גריפי פעיל ואפקטים מתקדמים , אשר אינם כוללים בתקון הHTML הבסיסי , כמו מצגות FLASH & JAVA , אבל בזמן האחרון השימוש תוספים הפחית בגלל העידכונים והחידושים שהוצגו ב5HTML וחוסר תמיכה בתוספים במכישירי המובייל .
כדי לאפשר לגלוש התמצאות נוחה באתר , ככה שיגיע במאמץ מזערי לכל אחד מדפי האתר המעניינים אותו , עומדים לרשותו בדל כלל כלים לניווט באתר .

רוב הדפים של האינטרנט נגישים במישרין או בעקיפין מדף אחד מרכזי שקוראים לו "דף הבית"
* כמובן יש אתרים שהם דורשים הרשמה לאתר או תשלום כלשו כדי להיכנס או לגשת לאזורים מסוימים בתוך האתר .

לאתר האינטרנט יש כמה סיבות לבניה שלו :

- אתר אינטרנט הוא מעין מרכז עצבים דיגיטלי של מידע מקצועי וקישורים, אשר מתקיימים זה בעזרת קיומו של זה, נתמכים יחדיו לכדי מעגל שבתחילתו ובסופו נמצא אתר האינטרנט.

- יש את אפשריות הקידום מבחינת מנועי חיפוש כמול גוגל, בינג, גופ, 2 **find** וכו.. , הם תומכות קודם כל בתהליך של בניית אתרי אינטרנט מבוססי קידום , הוראות טכנולוכיות שמעביר המקדם לבונה האתר ובאותם אתרים ישנם מאמרים מקצועיים ושאר חומרים אשר נכבתו בעזרת הייעוץ והכוונה של מקדם אתרים .

- בניית אתרי אינטרנט מאפשרת איסוף והצגה מושלמת של חומרים שונים כגון מאמרים , תיק עבודות וסרטונים במקום אחד , תחת שם דומיין המייצג את עולם התוכן או את המצורצים שלו .

- אתר מקצועי וקל להבין אותו או לניווט, ידידותי למשתמש ומעוצב בהתאם למכשיר או לכלי שאנחנו נכניסים דרכיו במסודר ולפי ערכי עולם התוכן, זהו אתר אינטרנט אשר יצור טראפיק, שכאמור מביא להכנסה אשר מתורגמת לתזרים.

-דף עסקי בפייסבוק הוא כלי חשוב וממריץ לשם קידום יעיל ותגבור החשיפה , אך יש לשים לב לעובדה שזהו רק כלי כמו יצירת סרטונים, בניית דף נחיתה או השתתפות בפורומים וכתיבה לפורטלים כולם מקשרים בחזרה לאתר האינטרנט ומעניקים משקל כבד יותר לערכים ולמילות החיפוש בתהליך הקידום .

- איסוף מידע, קבלת חוות דעת ויצירת מאגר מסודר של הרבה לקוחות או מועדון לקוחות, מתאפשרים בעזרת פניה הכוללת מילוי טופס באתר עצמו או בעזרת בניית דף נחיתה, המקשר בחזרה אל הקטגוריה המבוקשת בתוך אתר האינטרנט עצמו.

- בהמשך לקודם – פילוח של קהל הלקוחות ופניות קבוצתיות מתוך מאגר הנתונים ושליחת ניוזלטרים לגבי עדכונים, חדשות ומבצעים או בקשה להירשם לשרות מסוים, מתאפשרים באתר.

- אתר אינטרנט הוא יישות דינאמית ולא חלל של בית עסק כלשהו, משמע, שינויים במבנה, החלפות תכנים או גרפיקה ואף החלפת מהות העסק ושרותיו (קניית דומיין חדש) – תמיד אפשריים .

- חשוב לדעת ולזכור : שאתר האינטרנט הוא נכס אישי לכל דבר, בית עסק אותו יש לתפעל מדי יום, לרענן תכנים, מוצרים ושרותים אחת לתקופה, להזמין אליו את הגולשים ולוודא שהינו חשוף ומקודם בערוצים הנכונים ללא קשר לקידומו במנוע החיפוש "כביול אסור לזייף דברים או להפיץ שקרים בדף האינטרנט שהם לא באמת , נגיד משהו שאנחנו מוכרים במחיר **X** , נפרסם אותו במחיר **Y** , זה יפגע לנו בעסק " .

- אתר האינטרנט שלכם הוא סיבה לגאווה, וודאו שאתם מדברים על האתר ועל התועלות שבתכניו בכל הזדמנות ובפני הקהל הומקום הנכון, שתפו וספרו עליו באתרי אינטרנט שונים עד כמה שמתאפשר אנשים קולטים בסביבה של מחויבות ותשוקה. צרו נוכחות באינטרנט בכך שירגישו אתכם באופן ממשי, ותפעלו רק מתוך הבנת הצרכים של קהל היעד.

תקיפה ה-SQL לאתרי האינטרנט :

הזרקה של ה-**SQL** היא מהדרכים הנפוצות ביותר לפריצה או תקיפה אתרי האינטרנט .

ביומינו עם ההתפתחות של האינטרנט , אתרי האינטרנט התחילו להתפתח יותר אתרים דינאמיים , אלה המיצגים מידע אישי לכל גולש לדוגמא אתרי הדואר כמו רשתות **Hotmail ,** **Gmail** וכו...

אתר דינאמי הוא נבנה באמצעות שימוש בכמה שפות תכנות , אלה פועולות בצד של השרת והם מבצעות עיבוד נתותים שונים ולבסוף שולחות את תוצאותם הסופית והיא מוצגת בצד המשתמש , לצורך הקמתו ותפעולו של אתר דינאמי צריך לשמור את הנתונים השונים , לכך משתמשים בביס נתונים .

בבסיס הנתונים הנפוצים ביותר הם בסיסי הנתנוים הטבלאים אלה ששומרים את המידע בטבלאות ותמוכים בגישה אליהם באמצעות שפת שאילתות מובנית , כמו **SQL(Structured Query Language)** שפתוחה על ידי **IMB** .

התקפת ההזרקה של **SQL** היא שיטה לניצול פריצה אבטחה בקוש של התוכנית .

בבתקפה מנצלת את שכבת בסיס הנתונים של היישום ומתרחשת כאשר המשתמש כותב נתונים לשדה קלט אליו אמורים היו להיכנס נתונים תמימים לכאורה למשל "שדה לקליטת שם או כתובת" , והם אינם מסוננים בצורה נכונה , באופן זה יכול משתמש זדוני לחרוג לחלוטין מהתבנית המקורית של שדה הקלט ולגרום על ידי הזרקת תווים שונים להצרת שאלילתות **SQL** על שרת הדאתאביס "**DB**" דרך דפי האינטרנט של ממשק ה "**WEB**" , בניגוד מוחלא לתכנון המקורי של האתר .

כל התוכניות שכוללות שאילתות ה **SQL** תוך שילוב של נתונים מהמשתמש , הם עלולות להיות פגיעות להזרקה ועשויים לחשוף את נתוניהם שהמתכנת עצמו לא חשב על זה שיוכלו להיחשף וזה יגרום נזק לנתותים עצמם , בנוסף לזה הזרקת ב **SQL** יכולה להוביל להתקפות אחרות בשל תצורה בעייתית של רשת האתר או בקרת הגישה היא חלשה . היא ניתנת למימוש באמצעות שמימוש אך ורק בדפדפן של האינטרנט (בלבד) .

- **יש כמה אפשריות להתגוננות מפני הזרקה/תקיפה SQL :**

1) באתרי אינטרנט אקטייבים צריך לבדוק את תקינות הקלט לפני שאנחנו משתמשים בו , מומלץ לאפס את כל קלט נתוני המשתמש בהתאם להקשר , לדוגמא בשדה לכתבות דואר האקטרוני יש לאפס ולאפשר מעבר רק לתווים החוקיים בדואר האקטרוני , בדה למספר טלפון יש לאפס ואפשר רק למספרים לעבור , והאלה ..
2) הגבלת את ההרשות של מסד הנתונים להקשר , יצירת חשבונות משתמש עם רמה מינימלת של הרשאות לסביבת השימוש שלהם , לודגמא , את הקוד שנמצא מאחורי דף כניסה צריך שנבצע שאילתת מסד נתונים באמצעות חשבון מוגבל רק לטבלה האישורים ששייכם לעניין (רלוונטיים) בדרך הזאת ההצלחה ההתקפה באמצע ערוץ זה לא יאפשר בהכרח פגיעה במסד הנתונים .
3) להימנע מבניית שאילתות של SQL עם קלט משתמש , כביכול שימוש במנגונים מובנים לבנית שאילתות סגורות . שימוש בשאילתות SQL כדי לקבל קלט משתמש עם פרצודורות מאוחסנות בזיכרון ללא שימוש בשאילות פתוחות הנבנות דינמית מקלט המשתמש .
4) להימנע מיכולת להכניס קבצים חיצוניים .
5) להשתמש בחומת אש ליישומי האינטרט שזה WAF (Web Application Firewall) .

כל אחת מאפשריות להתגוננות היא מפחיתה מאוד את הסיכוי להתקפת SQL מוצלחת . האפשריות האלה יספקו הגנה ברמה טובה מאוד ..

אני מצרף לכאן אתר/קישור שאפשר להיעזר בו גם שהוא בשפה לועזית :

https://crypto.stanford.edu/cs142/lectures/16-sql-inj.pdf

תקיפה ה -XSS :

תקיפה **XSS** היא תקיפה נגד גולשי האינטרנט המנוצלת באמצעות פגיעות ביישומי האינטרנט , והיא מאפשרת לתקוף ולהזריק סקריפט זדוני שהמטרה שלו היא לרוץ בדפדפנים של משתמשי מערכת אחרים .

בריצת הקוד יוכל התוקף לבצע פעולות בשמם של המשתמש בשירות דרך ניצול מוגבלות בפרוטוקול **HTTP** ולגנוב את מזהה המשתמש .

אז בעצם **XSS** זה פירצה מאפשרת לשתול קוד זדוני בתוך קישור תמים, או בתוך קובץ (תמונה למשל) שלא עובר בדיקת-תוכן.

הקוד הזדוני יכול לבצע מספר רב של פעולות כגון גניבת ה"עוגיה" (קובץ מיוחד הנשתל במחשבי הגולשים ומיועד לשמירת פרטי המשתמש לצורך זיהוי אוטומטי.
לקשר את האתר לכתובת אחרת.

בתחילת השימוש בשפת **JavaScript** הבינו שיש סכנה כאשר המשתמש מריץ קוד שנשלח אליו משרת האינטרנט , אחת הבעיות המרכזיות הייתה שלקוד זה הייתה גישה לכל החלונות הפתוחים באינטרנט(של הדפדפן), ובגלל זה אתר אינטרנט זדוני יכול היה לנסות לגנוב מידע שהמשתמש הכנס לאתרים אחרים שבמקרה היו פתוחים באותו זמן בחלונות אחרים בדפדפן , כדי לתקן את הבעיה הזו פותחה בדפדפני אינטרנט מדיניות "אותו מקור" .

במסגרת מדיניות זו קוד שנשלח מהשרת האינטרנט יכול לגשת רק למידע שמוקורו באתרים מאותו שם תחום על גבי פרוטוקול.

ככה אתרי אינטרנט זדוניים יכולים לגשת ק' למידע שהם עצמם ייצרו .

בכללי פרצות ה **XSS** לרוב מצלים אותם כדי לעקוף מדיניות הזאת . ניצול פרוצות מורכב ממציאת דרכים להכניס קוד זדוני לעמודים הקשורים לתחומים אחרים , ועל ידי כך יתן למנצל הפרצה גישה למידע רגיש אל אתרים האלה .

טבלה כלים שיימושים לבנית וקידום אתרים :

שם	מחיר	קטגוריה	מה הכלי עושה ?
AdWord & SEO Keyword Permutation Generator	חינם	מחקר מילות מפתח	מאפשר לכם לקחת 3 רמות של ביטויים ולחבר בניהם ליצירת לונגטייל מהיר ואיכותי
Website Penalty Indicator	חינם	טכני	מאפשר לדעת מאיזה עדכון נפגעתם
Microdata Generator	חינם	טכני	מאפשר להיכניס את כל הפרטים הלוקאלים של עסק ולייצר סכמה איכותית לצורך הטעמה באתר .
WooRank	חינם	טכני, אופטימיזציה	מנתח אתרים ברמה גבוהה מאוד
Free Broken Link Checker	חינם	קישורים פנייים	בודק את כל האתר ומוצא עבורכם קישורים שבוריים.
Browseo	חינם	טכני	המדמה התנהגות של הספיידר של גוגל ובכך מאפשר לנו לשפר את מבנה האתר שלנו
Soovle	חינם	מחקר מילות מפתח	מאפשר שימוש במשלים האוטומטי של מנועי החיפוש
Kolyom	**חינם**	בדיקת מיקומים	מאפשר בדיקת מיקומים בארץ הקודש בחינם
SEO Tools for Excel	חינם עם אופציות להוסיף פיצ'רים בתשלום	טכני, ניתוח קשרים	מאפשר לכם לנהל את כל מה שצריך לדעת על האתר בתוך אקסל ע"י שימוש בכלים
Website SEO Checker	חינם	טכני ניתוח קשרים	מאפשר לכם לבצע בדיקה של כמות עמודים בבת אחת ומיד לקבל את מדדי ה Page Authority + Domain Authority
Convert Word Documents to Clean HTML	חינם	תוכן	מאפשר להעתק את התוכן שכתבתם בוורד ולהמיר אותו לקוד HTML. בהחלט שימושי במקרים מסוימים.
Free Analysis of Your Google+ Page	**חינם**	**גוגל פלוס**	הכניסו את כתובת עמוד עסק הגוגל פלוס וקבלו רשימה של שיפורים שעליכם לעשות על מנת שהעמוד יהיה מושלם
Monitor Backlinks	החל מ 24.90$ בחודש **.** יש חודש התנסות בחינם	**קישורים**	מאפשר לבצע מעקב קישורים על האתר שלכם ואתרי מתחרים, לזהות את הקישורים הטובים והרעים (להערכת מפתחי הכלי) וגם לדעת מה המתחרים שלכם עושים. בנוסף, הכלי מאפשר לנטר אחר קישורים שבוצעו במסגרת החלפת קישורים או בניית קישורים.

-כלים/שיטות תקיפות נפוצות :

מול כל אחת מהשכבות הרשת יש מגוון גדול של טכניקות תקפיה , שיטות תקיפה נפוצות .

- זיוף כתובת **MAC** – בשכבת בקישוריות, **Data Link** , מיעון המסרים מתבצע על בסיס כתובת **MAC** , כתובת זאת מוטמעת על גבי כרטיסי הרשת או המודים כבר בשלב הייצור , טכניקות תקיפה של שכבה זאת כוללת זיוף כתובת **MAC** .
ניתן להפעיל טכניקה זו גם נגד מחשבים פייזים ובפרט נגד "מכונונות וירטואליות" .

- זיוף כתובת **IP** – ניתוב תעבורת הרשת באינטרנט ובמספר גדול של רשתות אחרות , מתבצע לפי כתובת לוגית שנקראת **IP**, כתובת זו אינה מוטמעת בציוד שלב הייצור , אלא כתובת לוגית שניתן לשנות אחת מטכניקות התקפיה כוללת אי זיופה.

- התקפת אדם באמצע – בשכבת ברשת התוקף מנתב את תעבורת הרשת כך שהיא תעבור "דרכיו" מבלי שאף אחד משני הצדדים מבחין בכך , מימוש התקפת אדם באמצע מפורסם ונפוץ הוא על ידי ביצוע מניפולציה על פרוטוקול .
להתמודדות מולה פותח מנגנון שנעזר ב "חתימה" של צד שלישי אמין תוך שימוש בהצפנה **HTTP Secure** .

- התקפת מניעת שירות - שיטת התקפה מאוד נפוצה שבה שולחים אל האתר שמארח את מתן השירות מספר של הודעות תוך זמן קצר ויוצרים עומס , כך גורמים לו להאט את הקצב שבו הוא יכול לתת מענה למשתמשים או אפילו מביאים לקריסתו .
- תקפת **XSS**- דיברנו עליה לפני זה והיא מאפשרת הזרקת קוד זדוני אל אתרי אינטרנט באמצעות הכנסת נתוני משתמש בעת הגלישה , שיטה זו משתמשת באמצע פיתוי על מנת שהיעד יגלוש באתק מסוים .

איך שומרים על אתרים וחשבונות מפריצות והשתלטות ?

יש כמה דרכים שיורידו את הסיכוי לפרוץ את האתר.

חלק גדול מאבטחת האתר נעשית על ידי בחירת ספק אינטרנט מתאים. יש לוודא שהספק מריץ ממקש ניהול טוב ועדכני, כמו **cPanel, Plesk** או **.H-sphere** כמן כן צריך לבדוק שגרסאות התוכנה, בעיקר **PHP, MySQL, Apache**מעודכנות לגרסאות אחרונות המסופקות ע"י מערכת ההפעלה או ממשק הניהול. באופן עקרוני אנו מעדיפים למקם אתרי **PHP** על שרתי לינוקס בגלל יכולת הפרדה ואבטחה טובה יותר. רצוי לבדוק עם הספק איזה מערכות אבטחה נוספות הוא מפעיל על השרתים ומחוץ להם **(mod_security, application firewall, IPS/IDS Systems**וחשוב מכל, איך מתבצעים הגיבויים ובמה כרוך שחזור אתר, באופן חלקי או מלא. השלב הבא ביצירת סביבה מוגנת הוא שמירה מתמדת על עדכון האפליקציה (וורדפרס, ג'ומלה, דרופל וכו.), כולל כל המרכיבים הנוספים כגון פלאגינים, תוספים, מודולים, תבניות, שפות וכל דבר אחר שהותקן באתר. יש לזכור שמדובר במערכות קוד פתוח וכולם יכולים לקרוא את הקוד ולאתגר את המתכנתים. רק שמירה מדוקדקת על עדכון האתר ימנע פריצה. ללא ביצוע עדכונים פירצה לאתר מבוסס קוד פתוח כמעט וודאית תוך 3 חודשים עד חצי שנה, חשוב לזכור את זה לפני שמתחילים לעבוד עם תוכנות קוד פתוח שפתוחות לאינטרנט. המחמירים ילכו ישנו שמות של קבצי קונפיגורציה נפוצים, כמו **config.ing.php** או **configuration.php**למשהו אחר, וכמו כן ישנו שמות של תיקיות אדמיניסטרציה, קידומות של טבלאות ויפעילו הגנת **IP** ו **basic authentication-**למערכות האדמין בנוסף למערכת האבטחה של האפליקציות עצמן**.**

- **בחירת סיסמא נכונה לשרותים השונים**

חלק חשוב בשמירה על בטיחות חשבון אחסון האתרים או השרת וירטואלי הוא קביעה, החלפה ושמירה על סיסמא חזקה ועדכנית. אנו ממליצים תחילה לבחור סיסמא שניתן לזכור. שנית, הסיסמא צריכה להיות חזקה ככל שהמערכת שמקבלת אותה יכולה. רוב המערכות יקבלו סיסמא של לפחות 8 תווים. נסו לייצר סיסמא שמורכבת ממילה אחת ארוכה או שתי מילים, בשגיאת איות אשר לא ניתנת למציאה מתוך מילון, יחד עם תו מיוחד, אות אחת גדולה לפחות ומספר. אם תשקיעו בזה כמה דקות המח שלכם יתחיל לייצר שמות לפחות כמו מחשבי הצבא עם "עופרת יצוקה" ו-"עמוד ענן". הנה שתי דוגמאות טובות **amud4An$; Hofer#et .:**נהוג להחליף סיסמא כל 3 חודשים לפחות. צוות סוויטהום כמעט לעולם לא יבקש את הסיסמא שלכם. גם אם מישהו יבקש, הוא ינחה אתכם לגשת לטופס יצירת הקשר באתר ולסמן את אופציית ההצפנה **(PGP)** לפני המשלוח. דבר חשוב אחרון – אל תשתמשו באותה סיסמה, או בשיטת קביעת סיסמה עקבית למערכות שונות. בחרו סיסמא ייחודית שלא ניתן לנחש בעזרת סיסמא אחרת שלכם. לאחרונה דלפו רשימות של שמות משתמשים וסיסמאות מאתרים שונים והבעיה התעצמה עם אנשים בעלי סיסמא זהה לדואר אלקטרוני, חשבון אחסון **PayPal ,**ועוד**.**

- **חיבור באמצעות פרוטוקול SSL לאתר אינטרנט**

סוויטהום מציעה לכל לקוח גישה לאתר שלו באמצעות פרוטוקול **.SSL** ראשי התיבות של **SSL** הן **.Secure Socket Layer**בעל האתר או חברת האחסון רוכשות מחברה מוכרת תעודה, אותה מתקינים על שרתי האינטרנט השונים וכשניגשים לאתר או לדואר באמצעות שם שרת תחת דומיין מוגן התעבורה בין השרת ללקוח מוצפנת. לסוויטהום דומיין ייחודי לצורך נושא זה **secured.co.il –** אשר תחתיו אנו מספקים קישורי "מראה" לאתרי הלקוחות. לקוח על שרת **cpanel** יקבל לינק בצורת **https://cpanelX.secured.co.il/~username**ולקוח על שרת **H-sphere** יקבל קישור בצורה **https://CUSTOMNAME.secured.co.il –**כאשר **CUSTOMNAME** ניתן לקביעה ע"י הלקוח. כמו כן חלק משרתי ה **FTP-**ניתנים לחיבור באמצעות **SSL** וכן כל הפרוטוקולים של דואר אלקטרוני

ניתנים לגישה ב **.SSL-**אנו ממליצים להגן על איזורי אדמיניסטרציה, כניסת לקוחות וכל מקום אחר שגולשים רגילים לא צריכים להסתובב בו ב **,SSL-**אפילו שיתופי. לקוחות עסקיים, אשר רכשו כתובת **IP**יעודית יכולים להתקין תעודות פרטיות, הניתנון לרישום אצל ספקי תעודות רבים בחשבון אחסון האתרים שלהם. ממשקי הניהול מאפשרים הכנת בקשת תעודה **CSR –** וסוויטהום תשמח להנפיק עבורכן מבחר תעודות במחירים מיוחדים ללקוחותיה**.**

- **אבטחת חלקי אדמיניסטרציה באתר באמצעות שם משתמש וסיסמה**

סוויטהום מאפשרת להציב הגנה על תיקיות בתוך חשבון האחסון שלך, הן על שרתי לינוקס והן על שרתי ווינדוס. הרבה מערכות מספקות לוגין מרוכז לגולשים ולמנהלים. בפועל מתגלות עם הזמן פרצות אבטחה, חלקן מתבאות בעקיפת בדיקת **session**או עקיפת מנגנוני האבטחה של האפליקציה בדרכים אחרות. במצב זה, הגנה נוספת ברמת **Basic Authentication** תמנע את ההתקפה מכיוון שהפורץ יצטרך בנוסף פרטי גישה או לפרוץ לשרת **.Apache** אם הוא יודע לפרוץ **Apache** מעודכן כנראה שהאתר שלך ממש מעניין האקר ברמה בינלאומית, הצלחת בגדול :) ממשקי הניהול שלנו מגיעים עם שלל כלים להגדרת הגנה על תיקיות, כולל שרתי ה **Windows-**אשר עושים זאת בצורה יפה ונקיה ע"י תוסף **ISAPI** המדמה התנהגות של קבצי **htaccess.** על שרתי לינוקס/אפאצ'י**.**